REMARKS

The Examiner rejected claims 1-2, 5 and 8-10 under 35 U.S.C. §103(a) as allegedly being unpatentable over Freivald et al. (US Patent Number 6,012,087), and further in view of Shanklin et al. (US Patent Number 6,487,666), as evidenced by Chari et al. (US Patent Number 6,425,006).

The Examiner rejected claims 3, 6 and 11 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Freivald and Shanklin, and further in view of Lunt (Detecting Intruders in Computer Systems).

The Examiner rejected claims 4, 7 and 12 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Freivald and Shanklin, and further in view of Martin et al. (US Patent Number 6,772,349).

Applicants respectfully traverse the §103 rejections with the following arguments.

09/966,227   7

35 U.S.C. §103(a)

The Examiner rejected claims 1-2, 5 and 8-10 under 35 U.S.C. §103(a) as allegedly being unpatentable over Freivald et al. (US Patent Number 6,012,087), and further in view of Shanklin et al. (US Patent Number 6,487,666), as evidenced by Chari et al. (US Patent Number 6,425,006).

Applicants respectfully contend that claims 1-2, 5 and 8-10 not unpatentable over Freivald, and further in view of Shanklin, as evidenced by Chari, because Freivald, and further in view of Shanklin, as evidenced by Chari does not teach or suggest each and every feature of claims 1-2, 5 and 8-10 . For example, Freivald, and further in view of Shanklin, as evidenced by Chari does not teach or suggest the feature: "altering an element of a signature set of the intrusion detection system responsive to an outcome of the step of comparing" (claims 1 and 8); "when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of the intrusion detection sensor to decrease an alert generation rate of the intrusion detection sensor" (claims 2, 5, 9-10).

The Examiner argues that "Freivald disclosed ... responsive to an outcome of the step of comparing (See Freivald Col. 13 Lines 29-37) (Also see Figure 14)".

In response, Applicants respectfully contend that Freivald teaches in steps 92, 91, 94 of FIG. 14 (as well as in col. 13, lines 29-37) that the ignore-signature flag is set if: 1) the number of notifications exceed a threshold value in step 92 AND 2) a last-modified header is found in step 91. Freivald most certainly does not teach setting the ignore-signature flag if the number of notifications exceed a threshold value. In other words, the number of notifications exceeding a threshold value is a necessary condition, but not a sufficient condition, for setting the ignore-

09/966,227   8

signature flag.

The following hypothetical example further illustrates the Examiner's incorrect use of logic. Consider a hospital having a rule that patients are generally served lunch at 11AM and that a diabetes patient in particular is served a sugar-free lunch at 11AM. The Examiner's logic would argue that the hospital rule teaches serving a sugar-free lunch to a patient at 11AM, which is of course incorrect since the hospital rule of serving a sugar-free lunch is specific to diabetes patients.

Similarly, the Examiner's argument that Freivald teaches setting the ignore-signature flag if the number of notifications exceed a threshold value is incorrect, since Freivald's teaching of setting the ignore-signature flag is specific to finding a last-modified header in step 91.

In addition, Applicants contend that the Examiner's argument for modifying Freivald by utilizing the alleged intrusion detection system of Shanklin is not persuasive. The Examiner argues: "It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the network intrusion detection system of Shanklin in the alert squelching system of Freivald, by utilizing the squelching system to lower the alert generation rate of the intrusion detection system.... This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that the system manager of an intrusion detection system was not overwhelmed by alerts, as well as ensuring that the network was not bottlenecked with alerts."

In response, Applicants note that the preceding Examiner's argument is based solely on the Examiner's speculation and personal opinion. The Examiner has not provided any evidence

09/966,227   9

from the prior art (as required by law for establishing a *prima facie* case of obviousness) demonstrating that "the ordinary person skilled in the art would have been motivated to ensure that the system manager of an intrusion detection system was not overwhelmed by alerts, as well as ensuring that the network was not bottlenecked with alerts".

Also in response, Applicants contend that the Examiner's argument of an alleged advantage of the system manager of an intrusion detection system not being overwhelmed by alerts is not applicable to Freivald, since Freivald's invention does not use an intrusion detection system. The Examiner appears to be using circular reasoning in arguing that Freivald should use an intrusion detection system to "ensure that the system manager of an intrusion detection system was not overwhelmed by alerts", which does not make any sense and is not persuasive.

In addition with regard to claims 5 and 10, Freivald, and further in view of Shanklin, as evidenced by Chari does not teach or suggest the feature: "when the value of the signature event counter exceeds the signature threshold quantity, generating an alert, recording a time of generating the alert in a **log**, determining from contents of the **log** a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold" (emphasis added).

The Examiner argues that "Freivald disclosed ...recording the time of the alarm in a log (See Freivald Col. 3 Lines 18-20, and Col. 7 Lines 39-41), using the log to determine the alert generation rate (See Freivald Col. 13 Lines 11-15)".

In response, Applicants maintain that the Examiner's citations in Freivald do not teach or suggest said feature of claims 5 and 10, because a log is not disclosed in the Examiner's citations

09/966,227   10

in Freivald.

Based on the preceding arguments, Applicants respectfully maintain that claims 1-2, 5 and 8-10 are not unpatentable over Freivald, and further in view of Shanklin, as evidenced by Chari, and that claims 1-2, 5 and 8-10 are in condition for allowance.

The Examiner rejected claims 3, 6 and 11 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Freivald and Shanklin, and further in view of Lunt (Detecting Intruders in Computer Systems).

Since claim 3 depends from claim 2, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 3 is not unpatentable over the combination of Freivald and Shanklin and further in view of Lunt.

Since claim 6 depends from claim 5, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 6 is not unpatentable over the combination of Freivald and Shanklin and further in view of Lunt.

Since claim 11 depends from claim 10, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 11 is not unpatentable over the combination of Freivald and Shanklin and further in view of Lunt.

The Examiner rejected claims 4, 7 and 12 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Freivald and Shanklin, and further in view of Martin et al. (US Patent Number 6,772,349).

09/966,227   11

Since claim 4 depends from claim 2, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 4 is not unpatentable over the combination of Freivald and Shanklin and further in view of Martin.

Since claim 7 depends from claim 5, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 7 is not unpatentable over the combination of Freivald and Shanklin and further in view of Martin.
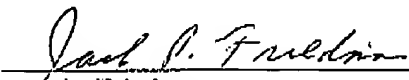
Since claim 12 depends from claim 10, which Applicants have argued *supra* to not be unpatentable over Freivald, and further in view of Shanklin, Applicants maintain that claim 12 is not unpatentable over the combination of Freivald and Shanklin and further in view of Martin.

09/966,227   12

CONCLUSION

Based on the preceding arguments, Applicants respectfully believe that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicants invites the Examiner to contact Applicants' representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account No. 09-0457.

Date: 02/01/2005

Jack P. Friedman
Registration No. 44,688

Schmeiser, Olsen & Watts
3 Lear Jet Lane, Suite 201
Latham, New York 12110
(518) 220-1850

09/966,227   13